NUI Galway
OÉ Gaillimh

Autumn Examinations 2015/ 2016

Exam Code(s)	4BCT1, 1SWB1
Exam(s)	Year 4 BSc in Computer Science and Information Technology, Science without Borders
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes		No	X

PTO

1

(a) What is meant by the term ‘block cipher’? (4 marks)

(b) 'Block ciphers are found with many modes of operation such as Cipher Feedback Mode, Cipher Block Chain, and Counter Mode.’ Give an account of the Cipher Block Chain mode of operation (6 marks)

(c) Discuss the security elements that are present in any online student service with which you are familiar (10 marks)

2

(a) ‘Public-key systems often depend on the apparent hardness of certain problems.’ Explain what is meant by this statement (4 marks)

(b) In the context of public-key cryptography, explain what is meant by the terms ‘registration authority’, ‘revocation list’ and ‘certification authority’. (6 marks)

(c) Alice is working on an assignment for her tutor Emma. Alice signs her assignment with her private signing key. Alice then encrypts this with Bob’s public encryption key and sends the assignment to Bob (who is in her class) for comment. Bob finds errors but instead of returning the assignment, he encrypts the signed assignment with Emma’s public encryption key and sends it on to Emma. So Alice signed it, but Bob sent it. Outline two approaches to dealing with this situation. (10 marks)

3

(a) ‘Two-factor authentication can be more secure than single factor.’ Briefly outline what is meant by two-factor authentication. (6 marks)

(b) ‘Nonce mechanisms provide freshness’. Explain how nonce mechanisms work. (6 marks)

(c) Give your understanding of the principles behind ‘zero-knowledge entity authentication’, using any analogy of your choice to illustrate your answer. (8 marks)

PTO

4

(a) Explain what is meant by the terms (1) Data origin authentication (2) Non-repudiation (6 marks)

(b) Give an account of the any one challenge-response scheme (for example, a login session with a bank or an authorisation via a payment card) with which you are familiar. (8 marks)

(c) What type of access environment might be expected to enforce 'no write up' and 'no read down' modes of operation between subjects and objects? Explain what is meant by 'no write up' and 'no read down' in the course of your answer. (6 marks)

5

(a) List any three challenges for cloud forensics (8 marks)
(b) Explain the relevance of the so-called 'Daubert Criteria' in computer forensics (6 marks)
(c) A laptop that has been returned by an employee now has a steganographic program on it. This was not there when the machine was released. In your opinion does this situation warrant further investigation? (6 marks)

6

"Information that people imagine to be private is increasingly available through social networking environments and search engines. Sometimes this information can even be changed". Discuss this statement from the perspectives of confidentiality (7 marks), integrity (7 marks) and availability (6 marks).